

REMARKS

In response to the Office Action dated December 17, 2004, Applicant respectfully requests reconsideration of the rejections of the claims. The withdrawal of the previous grounds of rejection, based upon the Baumann patent, is noted with appreciation.

Claims 1-3, 10 and 13 were rejected under 35 U.S.C. § 103, on the grounds that they were not considered to be patentable over the newly-cited Huff et al. patent (US 6,408,391) in view of the previously-cited Vaidya patent. The other pending claims were rejected on the basis of these two patents, in further view of the Hopkins reference. For the reasons presented below, it is respectfully submitted that these references do not teach the claimed subject matter to a person of ordinary skill in the art, whether considered individually or in combination.

With respect to claims 1-3, 10 and 13, the Office Action asserts that the Huff patent discloses all of the subject matter recited in these claims, with the exception of the creation of an attack model. To this end, the rejection refers to the Vaidya patent as teaching such a concept, and contends that it would obvious to include the creation of an attack model in the countermeasure system of the Huff patent. It is respectfully submitted, however, that the Vaidya patent does not disclose the creation of an attack *model*.

The rejection refers to the Vaidya patent at column 7, lines 36-37 and 42-45, as teaching the creation of an attack model. These portions of the patent refer to "attack signature profiles." It is respectfully submitted that an attack *signature*, per se, is not the same as an attack *model*. In the context of the present invention, an attack model can be used to generate a signature. See, for example, page 15, lines 4-6, as well as Figure 4, elements 70 and 72. As can be seen therefrom, a signature is distinct from the attack model itself.

In the disclosed embodiment of the present invention, the attack model includes an identification of a plurality of different types of hostile events, and manifestations of network events that are associated with each. See, for example, Table 3 on page 17 of the specification.

It is respectfully submitted that the Vaidya patent does not disclose a model of this nature.

Rather, it only discloses individual signature profiles. For example, at column 7, lines 42-45 (referenced in the Office Action), the attack signature profile merely determines whether the source address for a data packet is user Z. There is no association between this event and a particular type of attack, or any other information of relationships that would constitute a model.

Furthermore, claim 1 recites that the attack model is created by "analyzing and evaluating the knowledge base." The Office Action does not identify how the Vaidya patent can be interpreted to disclose this subject matter. In particular, it does not identify any portion of the patent that discloses a knowledge base of anomalous activity, let alone the creation of an attack model from such a knowledge base. Accordingly, it is respectfully submitted that the Vaidya patent does not disclose the concept of analyzing and evaluating a knowledge base to create an attack model. Consequently, even if the teachings of the Vaidya patent are applied to the countermeasure system of the Huff patent, the resultant combination would not be the same as the presently claimed subject matter.

With respect to claims 4-9, 11, 12, 14 and 15, the Office Action alleges that it would obvious to apply the teachings of the Huff and Vaidya patents to the specific types of wireless networks defined in these claims, in view of the Hopkins reference. However, the Office Action does not provide any motivation for combining the references in such a manner, absent knowledge of the present invention.

MPEP section 2143 sets forth the three basic criteria that must be met to establish a *prima facie* case of obviousness. The first of the criteria is that "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings." This section of the Manual goes on to state that the teaching or suggestion to make the claim

combination "must" be found in the prior art, "not in Applicant's disclosure." It is respectfully submitted that the rejection does not meet these requirements. In particular, it does not identify any relationship between the Huff and Vaidya patents, on one hand, and the Hopkins reference, on the other hand, that would lead a person of ordinary skill in the art to combine their teachings. Both the Huff and Vaidya patents are concerned with intrusion of *computer* networks, e.g. hacking or misuse by an unauthorized user. In contrast, the Hopkins reference is directed to the analysis of data link messages. Examples of these messages, set forth on page 1 of the reference, include position and velocity information of aircraft, as well as fuel data and weapons status of the aircraft. As set forth in the sentence bridging pages 3 and 4, the Hopkins reference is directed to a more intuitive analysis method for data link messages which is capable of providing speedier analysis. The Office Action does not identify any relationship between these objectives of the Hopkins reference and the intrusion detection systems of the Huff and Vaidya patents. The Hopkins reference does not contain any disclosure that "hacking" is a concern with the data link messages, nor otherwise suggest that the intrusion detection techniques of the other two patents are applicable thereto. It is respectfully submitted that, absent knowledge of the present application, there is no apparent motivation to combine the Hopkins reference with the Huff and Vaidya patents.

Furthermore, even if the references could be combined as suggested in the Office Action, a number of claimed features are not suggested by any such combination. For example, claim 4 recites that the wireless network is the Tactical Internet. As described in the present application, at page 2, lines 10-11, the Tactical Internet is a limited version of the Internet specially adapted for use by military units in the field. While the Hopkins reference refers to tactical data link messages, it does not disclose the Tactical Internet. For similar reasons, it does not disclose the subject matter of claim 14.

Claim 5 recites that the wireless network is a situation assessment data link (SADL).

Again, the Hopkins reference does not contain any disclosure of this claimed feature.

For at least the foregoing reasons, it is respectfully submitted that the subject matter of original claims 1-15 is not suggested by the Huff, Vaidya and Hopkins references, whether considered individually or in combination. For similar reasons, it is respectfully submitted that new claims 16-24 are likewise patentable over the disclosures of these references.

Reconsideration and withdrawal of the rejections and allowance of all pending claims are respectfully requested.

Respectfully submitted,
BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: March 17, 2005

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620